Introducción a la correspondencia entre pruebas y programas:

Principios del intuicionismo y del constructivismo

Alexandre Miquel

marzo de 2021

Una disyunción sin alternativa

Teorema

Al menos uno de los dos números $e+\pi$ y $e\pi$ es trascendente

Demostración.

Por el absurdo: Supongamos que $S = e+\pi$ y $P = e\pi$ son algebraicos. Entonces e, π son soluciones del polinomio con coeficientes algebraicos

$$X^2 - SX + P = 0\,.$$

Luego e y π son algebraicos. Contradicción.

- La prueba no dice quien de $e+\pi$ y/o de $e\pi$ es trascendente
  (La trascendencia de $e+\pi$ y de $e\pi$ todavía está conjeturada.)
- Carácter no constructivo viene del razonamiento por el absurdo

Una existencia sin testigo

Teorema

Existen dos números irracionales a y b tales a^b es racional.

Demostración.

O bien $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$, o bien $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$, por el tercer excluido. Dos casos:

- Si $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$, tomar $a = b = \sqrt{2} \notin \mathbb{Q}$.
- Si $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$, tomar $a = \sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$ y $b = \sqrt{2} \notin \mathbb{Q}$, pues:

$$a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = (\sqrt{2})^{(\sqrt{2}\times\sqrt{2})} = (\sqrt{2})^2 = 2 \in \mathbb{Q}$$

- La prueba no dice quien de $(\sqrt{2}, \sqrt{2})$ o $\left(\sqrt{2}^{\sqrt{2}}, \sqrt{2}\right)$ es solución
- Carácter no constructivo de la prueba viene del tercer excluido
- También hay pruebas constructivas (con $a = \sqrt{2}$ y $b = 2\log_2 3$)

La primera prueba no constructiva

- El tercer excluido y el razonamiento por el absurdo eran conocidos desde la Edad Antigua (Aristóteles). Sin embargo, nunca fueron usados de modo esencial antes del fin del siglo 19. Por ejemplo:

Teorema

Existen números trascendentes

Demostración constructiva, por Liouville 1844

El número $a = \sum_{n=1}^{\infty} \frac{1}{10^{n!}} = 0,110001000000\cdots$ es trascendente.

Demostración no constructiva, por Cantor 1874

Como $\mathbb{Z}[X]$ es numerable, el conjunto $\mathbb{A}$ de los números algebraicos también es numerable. Pero el conjunto $\mathbb{R} \sim \mathfrak{P}(\mathbb{N})$ no lo es. Entonces el conjunto $\mathbb{R} \setminus \mathbb{A}$ de los números trascendentes no es vacío, ni siquiera es numerable.

Plan

Plan

El intuicionismo de Brouwer

Luitzen Egbertus Jan **Brouwer** (1881–1966)

1908: *De onbetrouwbaarheid der logische principes*
(La desconfiabilidad de los principios de la lógica)

- Rechazo de principios no constructivos, tales como:
  - La ley del tercer excluido ($A \vee \neg A$)
  - El razonamiento por el absurdo (deducir A de la absurdidad de $\neg A$)
  - El axioma de elección, en sus formas más fuertes (Zorn, Zermelo)
- Principios del intuicionismo:
  - Filosofía del sujeto creativo
  - Cada objeto matemático es una construcción de la mente.
    Las pruebas también son construcciones (métodos, reglas...)
  - Rechazo del formalismo de Hilbert (lógica sin reglas)

Brouwer también hizo contribuciones fundamentales en topología clásica...
... para estar aceptado en el mundo académico matemático

La lógica intuicionista (LJ)

Aunque Brouwer era fuertemente opuesto al formalismo, las reglas de la lógica intuicionista (LJ) fueron formalizadas por su estudiante Arend **Heyting** (1898–1980)

1930: *The formal rules of intuitionistic logic*

1956: *Intuitionism. An introduction*

Intuitivamente:

- Las fórmulas $A \wedge B$ y $\forall x\, A(x)$ mantienen su sentido usual, pero las fórmulas $A \vee B$ y $\exists x\, A(x)$ adquieren un sentido más fuerte:
  - Una prueba de $A \vee B$ tiene que contener una prueba de A o de B
  - Una prueba de $\exists x\, A(x)$ tiene que contener un testigo x
- La implicación $A \Rightarrow B$ también adquiere un sentido algorítmico y la negación $\neg A$ (definida como $A \Rightarrow \bot$) ya no es involutiva

Técnicamente: LJ $\subset$ LK (LK = lógica clásica)

Lógica intuicionista: lo que se mantiene / lo que se pierde

- Se mantienen las implicaciones...

$$\begin{aligned} A &\Rightarrow \neg\neg A && \text{(Doble negación)} \\ (A \Rightarrow B) &\Rightarrow (\neg B \Rightarrow \neg A) && \text{(Contrarrecíproco)} \\ (\neg A \vee B) &\Rightarrow (A \Rightarrow B) && \text{(Implicación material)} \\ \neg A &\Leftrightarrow \neg\neg\neg A && \text{(Triple negación)} \end{aligned}$$

  pero las implicaciones recíprocas se pierden (salvo la última)

- Leyes de De Morgan:

$$\begin{aligned} \neg(A \vee B) &\Leftrightarrow \neg A \wedge \neg B & \qquad \neg(A \wedge B) &\Leftarrow \neg A \vee \neg B \\ \neg(\exists x\ A(x)) &\Leftrightarrow \forall x\ \neg A(x) & \qquad \neg(\forall x\ A(x)) &\Leftarrow \exists x\ \neg A(x) \end{aligned}$$

- **¡Cuidado!** No hay que confundir las reglas:

$$\frac{A \vdash \bot}{\vdash \neg A}\ \left(\begin{array}{c}\text{Introducción de la}\\ \text{negación, aceptada,}\\ \text{cf prueba de } \sqrt{2} \notin \mathbb{Q}\end{array}\right) \quad \text{y} \quad \frac{\neg A \vdash \bot}{\vdash A}\ \left(\begin{array}{c}\text{Razonamiento}\\ \text{por el absurdo,}\\ \text{rechazado}\end{array}\right)$$

Lógica intuicionista: lo que se mantiene / lo que se pierde

En álgebra:

- Se mantiene el álgebra elemental y abstracta
- La teoría del orden se mantiene (casi completamente)
- Lo mismo con la combinatoria

En topología:

- La topología tiene que ser completamente reformulada: topología sin puntos, espacios formales

En análisis:

- $\mathbb{R}$ todavía existe, pero ¡ya no es único! (Depende de la construcción)
- Funciones sobre conjuntos compactos ya no alcanzan su máximo
- Se puede reformular la teoría de la medida et de la integración de Lebesgue, pero con la construcción adecuada de $\mathbb{R}$ [Coquand'02]

Tercer excluido y decidibilidad

- Los intuicionistas no rechazan los enunciados de la forma $A \vee \neg A$. Éstos sólo tienen que ser demostrados... constructivamente
  - LJ $\vdash$ $(\forall x, y \in \mathbb{N})(x = y \vee x \neq y)$ (igualdad decidible en $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$)
  - LJ $\nvdash$ $(\forall x, y \in \mathbb{R})(x = y \vee x \neq y)$ (igualdad indecidible en $\mathbb{R}$, $\mathbb{C}$)
- Más generalmente, la fórmula $(\forall \vec{x} \in S)\,(A(\vec{x}) \vee \neg A(\vec{x}))$ significa: "La relación A es decidible en S"
- Dicha noción de "decidibilidad" se puede relacionar formalmente con la noción usual (i.e. computacional) de decidibilidad mediante el teorema de eliminación de cortes o la teoría de la realizabilidad
- **Variante:** Tricotomía
  - LJ $\vdash$ $(\forall x, y \in \mathbb{N})(x < y \vee x = y \vee x > y)$
  - LJ $\nvdash$ $(\forall x, y \in \mathbb{R})(x < y \vee x = y \vee x > y)$, pero:
  - LJ $\vdash$ $(\forall x, y \in \mathbb{R})(x \neq y \Rightarrow x < y \vee x > y)$

La jungla de las teorías intuicionistas

- Al nivel más elemental, el intuicionismo está bien definido:
  - LJ: Lógica intuicionista (de predicados)
  - HA: Aritmética de Heyting (= aritmética intuicionista)
  - + algunas extensiones estándar de HA (principio de Markov)
- Pero cuando se consideran teorías más sofisticadas, lo que es una teoría intuicionista es menos claro. Hay dos tendencias:
- **Teorías predicativas:** ("escuela sueca")
  - Análisis constructivo de Bishop
  - Teorías de tipos de Martin-Löf (MLTT)
  - Teoría constructiva de conjuntos de Aczel (CZF)
- **Teorías impredicativas:** ("escuela francesa")
  - El sistema F de Girard
  - El cálculo de construcciones de Coquand-Huet
  - El asistente de pruebas Coq
  - Zermelo-Fraenkel intuicionista (IZF_R, IZF_C) [Myhill-Friedman 1973]

Las contribuciones de Brouwer en la matemática clásica

Brouwer también hizo algunas contribuciones fundamentales en topología clásica, en particular en la teoría de las variedades topológicas:

Teorema (Punto fijo)

Toda función continua $f : D^n \to D^n$ tiene punto fijo $\quad (D^n =$ bola unidad de $\mathbb{R}^n)$

Teorema (Invarianza del dominio)

Sea $U \subseteq \mathbb{R}^n$ un conjunto abierto, con una función $f : U \to \mathbb{R}^n$ continua.
Si f es inyectiva, entonces $f(U)$ está abierto y la función f está abierta.

Corolario (Invarianza topológica de la dimensión)

Sean $U \subseteq \mathbb{R}^n$ y $V \subseteq \mathbb{R}^m$ conjuntos abiertos no vacíos
Si U y V son homeomorfos, entonces $n = m$.

... pero estos resultados usan razonamientos clásicos de modo esencial, y nunca fueron considerados como válidos por Brouwer

Plan

¿Qué es una teoría constructiva? (1/2)

- Ningún criterio formal para decir si una teoría $\mathscr{T}$ es constructiva, pero una mezcla de criterios sintácticos, semánticos y filosóficos
- Sin embargo, $\mathscr{T}$ tiene que cumplir al menos 4 criterios:

(1) $\mathscr{T}$ tiene que ser recursiva. Es decir: los conjuntos de derivaciones y de teoremas de $\mathscr{T}$ tienen que ser recursivamente enumerables

Obs.: Ya es el caso de las teorías clásicas estándar: PA, ZF, ZFC, etc.

(2) $\mathscr{T}$ tiene que ser consistente: $\mathscr{T} \nvdash \bot$

(3) $\mathscr{T}$ tiene que cumplir la propiedad de la disyunción:

Si $\mathscr{T} \vdash A \vee B$, entonces $\mathscr{T} \vdash A$ o $\mathscr{T} \vdash B$

(donde A y B son fórmulas cerradas)

(4) $\mathscr{T}$ tiene que cumplir la propiedad de la existencia numérica:

Si $\mathscr{T} \vdash (\exists x \in \mathbb{N})\, A(x)$, entonces $\mathscr{T} \vdash A(n)$ para algún $n \in \mathbb{N}$

(donde $A(x)$ sólo depende de x)

¿Qué es una teoría constructiva? (2/2)

- El la mayoría de las casos, también se requiere que:

  (5) $\mathscr{T}$ tiene que cumplir la propiedad de la existencia (o del testigo):

Si $\mathscr{T} \vdash \exists x\, A(x)$, entonces $\mathscr{T} \vdash A(t)$ para algún término t

(donde $A(x)$ sólo depende de x)

Obs.: Este criterio tiene que ser adaptado cuando el lenguaje de $\mathscr{T}$ no tiene términos cerrados, por ejemplo: la teoría de conjuntos

Teorema (No constructividad de las teorías clásicas)

Si una teoría clásica es recursiva, consistente y contiene Q, entonces no cumple ni la propiedad de la disyunción ni la de la existencia numérica

Obs.: Q = Aritmética de Robinson = fragmento de PA en que el esquema de inducción ha sido remplazado por el axioma (mucho más débil) $\forall x\,(x = 0 \vee \exists y\,(x = s(y)))$

Demostración. Por el primer teorema de incompletitud de Gödel, $\mathscr{T}$ es incompleta y existe una fórmula cerrada G tal que $\mathscr{T} \nvdash G$ y $\mathscr{T} \nvdash \neg G$. Se concluye observando que:

$$\mathscr{T} \vdash G \vee \neg G \qquad \text{y} \qquad \mathscr{T} \vdash (\exists x \in \mathbb{N})\,((x = 1 \wedge G) \vee (x = 0 \wedge \neg G))$$

¿Por qué LJ no garantiza el carácter constructivo? (1/3)

- El constructivismo es un criterio semántico (y filosófico), que no se puede garantizar sólo por el uso de la lógica intuicionista (LJ)
- De hecho, axiomatizaciones burdas en LJ pueden implicar el tercer excluido, y luego inducir teorías no constructivas. Algunos ejemplos:
- **En la aritmética intuicionista (HA):**
  - El axioma del buen orden

$$(\forall S \subseteq \mathbb{N})\,[\exists x\,(x \in S) \;\Rightarrow\; (\exists x \in S)(\forall y \in S)\, x \leq y]$$

    implica el tercer excluido; no es constructivo. En HA, el principio de inducción (que es constructivo) no implica el buen orden

¿Por qué LJ no garantiza el carácter constructivo? (2/3)

- **En análisis constructivo:** [Bishop 1967]
  - El axioma de tricotomía

    $$(\forall x, y \in \mathbb{R})\,(x < y \vee x = y \vee x > y)$$

    no es constructivo. Tiene que ser remplazado por el axioma

    $$(\forall x, y \in \mathbb{R})\,(x \neq y \Rightarrow x < y \vee x > y)$$

    que es clásicamente equivalente

  - El axioma de completitud

    > Todo subconjunto no vacío y superiormente acotado en $\mathbb{R}$ tiene supremo en $\mathbb{R}$

    implica el tercer excluido. El axioma de completitud tiene que ser restringido a los subconjuntos $S \subseteq \mathbb{R}$ que cumplen la propiedad:

    $$(\forall a < b \in \mathbb{R})\ ((\forall x \in S)\,(x \leq b)\ \vee\ (\exists x \in S)\,(x \geq a))$$

    (los conjuntos "order located above" en inglés)

¿Por qué LJ no garantiza el carácter constructivo? (3/3)

- **En teoría de conjuntos intuicionista:**
  - La formulación estándar del axioma de fundación

    $$\forall x\,(x \neq \varnothing \Rightarrow (\exists y \in x)(y \cap x \neq \varnothing))$$

    implica la ley del tercer excluido. Dicho axioma tiene que ser remplazado por el esquema de inducción conjuntista

    $$\forall x\,((\forall y \in x)\,A(y) \;\Rightarrow\; A(x)) \;\Rightarrow\; \forall x\,A(x)$$

    que es clásicamente equivalente al axioma de fundación
  - El axioma de elección conjuntista (Zorn, Zermelo, etc.) también implica la ley del tercer excluido [Diaconescu 1975]
- Siempre se demuestra que una teoría intuicionista es constructiva usando técnicas de eliminación de cortes o de realizabilidad

Algunas teorías constructivas

Teorías predicativas:

- Aritmética de Heyting (HA)
- Teoría(s) de tipos de Martin-Löf (MLTT)
- Zermelo-Fraenkel constructivo (CZF)

Teorías impredicativas:

- Aritmética intuicionista de segundo orden (HA2)
- Aritmética intuicionista de n-ésimo orden (HAn, con $n \geq 2$)
- Aritmética intuicionista de alto orden (HAω)
- Zermelo intuicionista (IZ)
- Cálculo de construcciones inductivas (Coq)
- Zermelo-Fraenkel intuicionista con remplazo (IZF$_R$)
- Zermelo-Fraenkel intuicionista con colección (IZF$_C$)